AD/COM

[redacted]

GPO PRICE $ ______

OTS PRICE(S) $ ______

Hard copy (HC) 2.00

Microfiche (MF) .50

ADCOM, INC.
808 Memorial Drive
Cambridge 39, Mass.
UN 8-7386

ADVANCED COMMUNICATION RESEARCH AND DEVELOPMENT

AD/COM

Second Quarterly Progress Report
for
COMMAND SYSTEM STUDY FOR THE OPERATION AND CONTROL OF UNMANNED SCIENTIFIC SATELLITES
Task II
Closed-Loop (Feedback) Verification Techniques
30 September 1964 - 31 December 1964

Contract No. NAS 5-9705

Prepared for

Goddard Space Flight Center
Greenbelt, Maryland

Submitted by

ADCOM, Inc.
808 Memorial Drive
Cambridge 39, Massachusetts

ADVANCED COMMUNICATIONS • RESEARCH AND DEVELOPMENT

AD/COM

Second Quarterly Progress Report
for
COMMAND SYSTEM STUDY FOR THE
OPERATION AND CONTROL OF
UNMANNED SCIENTIFIC SATELLITES
Task II
Closed-Loop (Feedback) Verification Techniques
30 September 1964 - 31 December 1964

Contract No. NAS 5-9705

Prepared for

Goddard Space Flight Center
Greenbelt, Maryland

by

J. Levy
A.M. Manders
S. M. Sussman

Approved by Elie J. Baghdady
Elie J. Baghdady
Technical Director

Submitted by

ADCOM, Inc.
808 Memorial Drive
Cambridge, Massachusetts

24998

ABSTRACT

24898

This report covers progress during the reporting period on the Command System Study for the Control of Unmanned Scientific Satellites under Task II Closed-Loop (Feedback) Verification Techniques. The report contains further analysis of feedback system performance, code structures and telemetry link adaptation.

Specific conclusions are:

a) One meaningful measure of error detection system performance is the probability, P_e, of an accepted codeword being in error. This error probability depends only on the uplink characteristics and on the code structure, but not on the feedback link. For a binary symmetric channel with transition probability p, P_e can be calculated from the codeword weight distribution, W(i), or from an approximation to W(i).

b) Cyclic codes for error detection can be altered to detect loss of synchronization by the addition of a fixed binary vector to each codeword prior to transmission. These codes are characterized by a pair of numbers $[s, \delta]$ such that a synchronization slip of s bits can be detected whenever each codeword contains less than δ errors. Multiple repetitions of cyclic codewords, appropriately altered, permit a considerable range of s and δ at some sacrifice in data rate.

c) Telemetry formats must be adapted to accept feedback information from the updata link. Feedback will, in general, demand only a small percentage of downlink capacity, but the allocation of this capacity will require appropriate design of telemetry formats to provide timely access to the downlink.

Author

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

LIST OF TABLES

I. INTRODUCTION

1.1 General

This report covers work during the second quarter on Task II of contract NAS 5-9705. A concurrent report on Task I entitled, "Unified Tracking/ Command/Telemetry at Lunar Distances," will be issued under separate cover. The objectives of Task II are:

To study command feedback/verification strategies in general. This will include code structures and synchronization in both directions, error detection and/or correction implementation, and system integration with emphasis on compatibility with GSFC equipment. Performance in terms of resultant data and command rates, command error probability, channel preemption, and other pertinent criteria will be presented. Adaptive techniques will also be studied. Recommendations of techniques suitable to specific type spacecraft missions will be made.

1.2 Summary of Work During Reporting Period

a) The analysis of a simple acknowledge/repeat-request feedback system is continued with a treatment of the probability of undetected error in Sec. 2.2.

b) A class of codes that provides reliable indication of loss of block synchronization as well as detection of errors is described in Sec. 2.3. These codes are simple alterations of cyclic codes. Design procedures and important properties of these codes are presented.

c) The operational considerations of incorporating updata feedback on telemetry links are discussed in Sec. 2.3. Methods applicable to existing telemetry formats are suggested.

II. DISCUSSION

2.1 Probability of Undetected Error for Feedback System

In the preceding Quarterly Report, a simple Acknowledge-Repeat Feedback System was analyzed and the relationship between the probabilities of missed command, $P_{m.c.}$, and unrequested repeat, $P_{u.r.}$, was derived. We turn now to the third type of malfunction: command conversion. The probability of command conversion, $P_{c.c.}$, was previously shown to be

$$P_{c.c.} = \frac{p_u}{1 - p_d q_r} < \frac{p_u}{1 - p_d} = \frac{p_u}{q_c + p_u} \qquad (2.1)$$

with the notation defined in Table I. $P_{c.c.}$ is the probability that a particular command during one of its repeat cycles is corrupted by an undetectable error pattern. A valid but incorrect command is then accepted at the spacecraft. Stated another way $P_{c.c.}$ is the fraction of transmitted commands (not counting repeats of the same command) that are erroneously accepted at the spacecraft.

$P_{c.c.}$ is one important measure of system performance, another one is the fraction of accepted commands that are erroneous. This fraction is the error rate P_e referred to accepted commands rather than to transmitted commands and is given by

TABLE I

Definitions of Probabilities for Simple Acknowledge-Repeat Feedback System

p_u		- undetected error
p_d		- detected error
p_e	$= p_u + p_d$	- error probability for the uplink
q_c	$= 1 - p_e$	- correct reception for the uplink
p_a		- acknowledgement transposed into repeat request
q_a	$= 1 - p_a$	- correct reception of acknowledgement
p_r		- repeat request transposed into acknowledgement
q_r	$= 1 - p_r$	- correct reception of repeat request

Note that error probabilities are denoted by p and correct reception probabilities by q.

$$P_e = \frac{P_{c.c.}}{1 - P_{m.c.}} = \frac{p_u}{1 - p_d q_r - p_d p_r} = \frac{p_u}{1 - p_d}$$

$$P_e = \frac{p_u}{q_c + p_u} = \frac{1}{(q_c/p_u) + 1} \qquad (2.2)$$

Note that P_e is exactly the upper bound on $P_{c.c.}$ and depends only on the uplink parameters, in particular, the ratio q_c/p_u.

It is of interest now to investigate the behavior of P_e as a function of the uplink channel characteristics. We assume the updata is encoded into blocks of length n using a code with a Hamming distance† distribution W(i). The function W(i) represents the number of codewords at a distance i from a particular codeword and is assumed to be the same for each codeword. For a group code the distance distribution is also the weight distribution, where the weight of a codeword is defined as the number of nonzero positions in a code block.

The number of codewords in the code is 2^k, i.e., each block contains k information digits. The sum of codewords at all distances i must equal 2^k, and since W(0) = 1 we have

$$\sum_{i=d}^{n} W(i) = 2^k - 1 \qquad (2.3)$$

where d is the minimum distance of the code.

† The Hamming distance between two codewords is number of positions in which the words differ.

The probability of undetected error p_u is the probability of an error pattern that converts the transmitted codeword into one of the other codewords at some distance i from the transmitted word. Assuming a binary symmetric channel having a transition probability p and a code with minimum distance d, we have

$$p_u = \sum_{i=d}^{n} W(i)\, p^i (1-p)^{n-i}. \tag{2.4}$$

The probability q_c of no errors in a block is given by

$$q_c = (1-p)^n \tag{2.5}$$

whereupon

$$\frac{p_u}{q_c} = \sum_{i=d}^{n} W(i) \left(\frac{p}{1-p}\right)^i \tag{2.6}$$

Since $[p/(1-p)]^i$ is a monotonically decreasing function of i for $p < \frac{1}{2}$, we have with the help of Eq. (2.3) upper and lower bounds

$$W(d) \left(\frac{p}{1-p}\right)^d < \frac{p_u}{q_c} < \left(\frac{p}{1-p}\right)^d \sum_{i=d}^{n} W(i) = \left(\frac{p}{1-p}\right)^d (2^k - 1) \tag{2.7}$$

Inserting these bounds into P_e gives

$$\frac{1}{\left(\frac{1-p}{p}\right)^d \frac{1}{W(d)} + 1} < P_e < \frac{1}{\left(\frac{1-p}{p}\right)^d \frac{1}{2^k - 1} + 1} \tag{2.8}$$

Under favorable channel conditions, i.e., $p \to 0$, use of the binomial expansion gives

$$\left(\frac{p}{1-p}\right)^d W(d)\left[1-\left(\frac{p}{1-p}\right)^d W(d)\right] < P_e < \left(\frac{p}{1-p}\right)^d (2^k-1) \tag{2.9}$$

with the lower bound yielding the better approximation for the limit $p \to 0$, viz.

$$P_e \approx p^d W(d) \tag{2.10}$$

At the other extreme, under poor conditions, the binary error probability p approaches one half. Therefore since $W(d) >> 1$ and $2^k-1 >> 1$, both bounds indicate $P_e \to 1$ as $p \to \frac{1}{2}$. This means that as the updata channel deteriorates, the ratio of erroneous accepted words to total accepted words approaches one.

It can be seen from Eq. (2.2) that

$$\lim_{q_c \to 0} P_e = 1, \tag{2.11}$$

holds in general and not only for the binary symmetric channel. The approach to the limit can be investigated by differentiating P_e with respect to p.

$$P_e = \frac{p_u/q_c}{1+(p_u/q_c)}$$

$$\frac{dp_e}{dp} = \frac{1}{[1+(p_u/q_c)]^2} \frac{d}{dp}(p_u/q_c)$$

$$= \frac{1}{[1+(p_u/q_c)]^2} \frac{1}{p(1-p)} \sum_{i=d}^{n} i\,W(i)\left(\frac{p}{1-p}\right)^i \tag{2.12}$$

In the limit when $p = \frac{1}{2}$ we have

$$\frac{p_u}{q_c} = \sum_{i=d}^{n} W(i) = 2^k - 1 \tag{2.13}$$

and

$$P_e \Big|_{p=\frac{1}{2}} = \frac{2^k - 1}{2^k} = 1 - 2^{-k} \tag{2.14}$$

The summation appearing in $\frac{dp_e}{dp}$ when $p = \frac{1}{2}$ is the average distance of the code. For group codes (a subclass of linear codes) the average distance or average weight is found to be[1]

$$2^{-k} \sum_{i=d}^{n} i\, W(i) = \frac{n}{2} \tag{2.15}$$

Consequently

$$\frac{dp_e}{dp} \Big|_{p=\frac{1}{2}} = 2n2^{-k} \tag{2.16}$$

A power series expansion of P_e at the point $p = \frac{1}{2}$ becomes

$$P_e \approx 1 - 2^{-k} - (1 - 2p)\, n2^{-k} \tag{2.17}$$

The behavior of P_e in this region is dominated by the exponential dependence on k, the number of information bits per block. For practical codes the block length n is considerably less than the number of codewords 2^k. To this order of approximation the behavior of p_e is not dependent explicitly on the minimum distance d. However, Eq. (2.17) is valid only near $p = \frac{1}{2}$; the approximation rapidly worsens as p decreases.

For the two extremes of very good and very poor channels Eqs. (2.10) and (2.17) respectively provide satisfactory estimates of p_e. Performance in the intermediate region can be determined by calculation of Eqs. (2.2) and (2.6) for specific codes.

An alternative ad hoc approximation has been suggested in Refs. 2 and 3 and checked with reasonable success on data transmitted over telephone channels. In this approximation it is assumed that the code detects all but a fraction $2^{-(n-k)}$ of the error patterns of weight greater than the minimum distance d. For the binary symmetric channel this means

$$p_u = 2^{-(n-k)} \sum_{i=d}^{n} \binom{n}{i} p^i (1-p)^{n-i} \tag{2.18}$$

Comparison with Eq. (2.4) shows that this approximation would be exact if

$$W(i) = \binom{n}{i} 2^{-(n-k)} \qquad d \leq i \leq n \tag{2.19}$$

However, even when Eq. (2.19) is not satisfied for all i, the sum in Eq. (2.18) may be a close approximation to the sum in Eq. (2.4).

An alternate approximation given in Ref. 4 takes the form

$$W(i) \approx \begin{cases} 2^{-(n-k)} \left[\binom{n}{i} - \binom{n-k}{i} \right], & d \leq i \leq (n-k) \\ \\ 2^{-(n-k)} \binom{n}{i} & n-k \leq i \leq n \end{cases} \tag{2.20}$$

but this differs insignificantly from Eq. (2.19).

The merit of approximations such as these is that the complete weight distribution of the code is not necessary for an estimate of performance. Exact weight distributions are known for only a handful of codes. Table II illustrates two of these from the Bose-Chandhuri-Hocquenhem class along with the corresponding approximation.

2.2 Cyclic Codes for Detecting Loss of Synchronization

2.2.1 Basic Definitions

It has been noted in the previous QPR (pp. 17-18) that cyclic codes, while possessing many properties making them desirable for the reliable transmission of command words in the presence of noise, are insensitive to loss of synchronization. In the following section we shall study a general procedure, easily implemented, which alters a cyclic code so as to give it the slip-detecting characteristic $[s, \delta]$. A code is defined to have the slip-detecting characteristic $[s, \delta]$ if for all overlap sequences caused by shifting the word frame s units or less from its correct location, the Hamming distance between the resulting overlap sequence and any valid word in the code is at least δ. (If $s = \langle n/2 \rangle$, the integer part of $n/2$, then the code is defined to be comma-free with degree of comma freedom δ.)

The ρ-repetition altered cyclic codes, a special class of comma-free codes which may be designed with arbitrary degree of comma freedom are introduced in Sec. 2.2.3. These codes appear promising for applications where there is need for a code combining error correction

TABLE II

Weight Distributions and Their Approximation for Two Bose-Chandhuri-Hocquenhem Codes. W(i) is Symmetrical about $i = \frac{n}{2}$; also W(1) = W(n) = 1.

i	W(i) (23, 12)	$\binom{23}{i}2^{-11}$	W(i) (31, 21)	$\binom{31}{i}2^{-10}$
5	0	0	186	166
6	0	0	806	719
7	253	120	2635	2568
8	506	239	7905	7704
9	0	399	18910	19688
10	0	559	41602	43313
11	1288	660	85560	82688
12	1288	660	142600	137813
13	0	559	195300	201419
14	0	399	251100	258967
15	506	239	301971	293496
16	253	120	301971	293496

with self synchronization capability, and where low code rates (0.10 - 0.30, typically) can be tolerated.

An (n, k) binary cyclic code consists of all polynomials which are multiples modulo $x^n + 1$ of a generator polynomial $g(x)$ dividing $x^n + 1$ and having coefficients in GF(2), the Galois field of two elements. The ith codeword is therefore expressible as $w_i(x) = g(x) \cdot a_i(x)$. $g(x)$ is of degree $n - k$; $a_i(x)$ is of degree $< k$.

A thorough description of the mathematical structure of cyclic codes is given in Ref. 1, Chap. 8. The following example will demonstrate in essence the mathematics of codeword generation. Let $g(x)$ be $1+x^2+x^3$ which is one of the factors of $x^7+1 = (1+x^2+x^3) \cdot (1+x^2+x^3+x^4)$. This polynomial generates the Hamming (7, 4) single-error-correcting code in cyclic form. We may generate codewords as shown below. Observe that multiplication and addition in GF(2) is identical to modulo 2 multiplication and addition.

$$g(x) \cdot 1 = 1 + x^2 + x^3 \qquad 0\ 0\ 0\ 1\ 1\ 0\ 1$$

$$g(x) \cdot x = x + x^3 + x^4 \qquad 0\ 0\ 1\ 1\ 0\ 1\ 0$$

$$g(x) \cdot (1 + x^2) = 1 + x^2 + x^3 + x^2 + x^4 + x^5$$

$$= 1 + x^3 + x^4 + x^5 \qquad 0\ 1\ 1\ 1\ 0\ 0\ 1$$

2.2.2 Analysis of Slip Detection

We shall concern ourselves in our analysis with codes derived from cyclic codes by the addition of a polynomial $r(x)$ to yield the new codeword $v_i(x) = g(x) \cdot a_i(x) + r(x)$. The polynomial $r(x)$ is of degree $<$n-k.

[If r(x) is of greater degree, then it can certainly be expressed as g(x) · b(x) + r'(x), where r'(x) is of degree $<n-k$. By virtue of the group property of the cyclic code, addition of r(x) creates a code equivalent to that created by addition of r'(x)]. Thus, if a code word is written with the k information digits occupying the places of x^{n-1}, x^{n-2}, . . . x^{n-k-1}, and the remaining n-k places filled with parity check digits, as may certainly be done, (Ref. 1, page 149), the polynomial r(x) will affect only parity digits. It will complement digits in those places in which r(x) has a "1", and leave untouched those places in which r(x) has a zero.

We shall now see how proper selection of r(x) is related to the slip-detecting characteristic (s, δ).

We shall, in this analysis, have occasion to refer to polynomials with indeterminate coefficients. It is therefore convenient to define $u_t(x)$ to be an indeterminate polynomial of degree $<t$, i.e., $u_2(x)$ may assume any of the values 1, x, 1 + x. $\phi_{(p-1)}(x)$ is an indeterminate polynomial of weight p - 1, and degree $<n$.

A code word is written as $b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \ldots + b_1x + b_o$. The highest order digits b_{n-1}, b_{n-2} . . . b_{n-k-1} are the information digits. Slips of t digits in the placement of the word frame, $t \leq < n/2 >$ must fall into one of two categories:

1. t highest order digits of a word cutoff; n-t lowest order digits of word fill n-t highest order positions of framed sequence; t highest order digits from another word fill in t lowest order places.

2. t lowest order digits of a word cutoff; n-t highest order digits of word fill n-t lowest order positions of framed sequence; t lowest order digits from adjacent word fill in t highest order places.

We may now write expressions for the indeterminate overlap sequences formed by type 1 and type 2 slips of t digits. It should be kept in mind that it is a property of modulo $x^n + 1$ polynomial algebra that $x^t \cdot v_i(x)$ is simply $v_i(x)$ cyclically upshifted t places. For example, modulo $x^7 + 1$:

$$1 + x^3 + x^4 + x^5 = 0\ 1\ 1\ 1\ 0\ 0\ 1$$

$$x^2(1+x^3+x^4+x^5) = x^2+x^5+x^6+x^7 = 1+x^2+x^5+x^6 \text{ modulo } x^7 + 1$$

$$= 1\ 1\ 0\ 0\ 1\ 0\ 1, \text{ which is } 0\ 1\ 1\ 1\ 0\ 0\ 1$$

cyclically shifted two places to the left.

Consider first a type 1 slip of t digits. The overlap sequence formed will be:

$$x^t v_i(x) + u_t(x) = x^t w_i(x) + x^t \cdot r(x) + u_t(x).$$

If the code is to be characterized by the self-synchronizing property (s, δ) then the distance between an overlap sequence of type 1 and a valid codeword $v_j(x)$ must be at least δ.

$$x^t v_i(x) + u_t(x) + v_j(x) + \phi_{(\delta-1)}(x) \neq 0. \qquad t = 1, 2, \ldots s$$

or

$$[x^t w_i(x) + w_j(x)] + r(x)[x^t + 1] + u_t(x) + \phi_{(\delta-1)}(x) \neq 0. \qquad t = 1, 2, \ldots s \qquad (2.21)$$

It is a property of the original cyclic code that if $W_i(x)$ is a codeword, $x^t \cdot w_i(x)$ must also be a codeword. Also, since a cyclic code is indeed a group code:

$$x^t w_i(x) + W_j(x) = W_\ell(x), \text{ another codeword.}$$

Thus, Eq. (2.21) may be rewritten as:

$$r(x)\,[x^t + 1] + u_t(x) + \phi_{(\delta - 1)}(x) \neq W_\ell(x) \qquad t = 1, 2, \ldots s \qquad (2.22)$$

where $W_\ell(x)$ is a codeword in the original cyclic code.

The consideration of type 2 slips in an analogous manner will also lead to Eq. (2.22). Thus, a code created by the addition of r(x) to all words from a cyclic code will have the slip-detecting characteristic (s, δ) if and only if Eq. (2.22) is satisfied.

We now note a condition upon r(x) which is a necessary condition for the solution of Eq. (2.22) but is not a sufficient condition.

Condition:

The minimum weight of that part of $r(x)\,[x^t + 1]$ involving degree of $x \geq t$; $t = 1, 2, \ldots s$, must be at least δ.

Explanation:

$u_t(x)$ may make equal to zero that part of $r(x)\,[x^t + 1]$ of degree $< t$. If the part of $r(x)\,[x^t + 1]$ having degree $\geq t$ has a weight of at least δ, then $\phi_{(\delta - 1)}(x)$ cannot wipe it out completely. Thus, the condition upon r(x) is necessary, since it insures that $r(x)\,[x^t + 1] + u_t(x) + \phi_{(\delta - 1)}(x)$

cannot equal the codeword of all 0's. It is not sufficient to guarantee that Eq. (2.22) is satisfied for the nonzero codewords. Below are tabulated some r(x) satisfying the above condition for arbitrarily large s. These values of r(x) can in no sense be considered "optimum". They have been discovered by a non-analytic procedure which may best be described as a series of educated guesses. Those r(x) denoted by an asterisk may be recognized to be Barker sequences.

δ	r(x)	z: degree of r(x)
1	1	0
2	$x+x^2$ (110)*	2
3	$1+x^2+x^3+x^4$ (11101)*	4
4	$x+x^4+x^5+x^6$ (1110010)*	6
5	$x+x^4+x^6+x^7+x^8$ (111010010)	8
6	$x^2+x^4+x^7+x^8+x^9+x^{10}$ (11110010100)	10
7	$1+x^2+x^4+x^5+x^8+x^9+x^{10}+x^{11}+x^{12}$ (1111100110101)	12
8	$x^2+x^4+x^6+x^7+x^{10}+x^{11}+x^{12}x^{13}x^{14}$ (111110011010100)	14
9	$x+x^4+x^6+x^8+x^9+x^{12}+x^{13}+x^{14}+x^{15}+x^{16}$ (11111001101010010)	16
10	$1+x+x^3+x^6+x^8+x^{10}+x^{11}+x^{14}+x^{15}+x^{16}+x^{17}+x^{18}$(1111100110101001011)	18

To find solutions to Eq. (2.22) it is necessary to put some specifications upon the structure of the cyclic code. Theorem I below indicates a method of construction of an interesting class of comma free codes having $\delta = 1$.

<u>Theorem I</u>: Let r(x) = 1 be added to each word of an (n, k) cyclic code having $k \leq < n/2 >$. The resultant code will be comma free with $\delta = 1$.

Proof: Writing down Eq. (2.22) with $r(x) = 1$, $\delta = 1$, $x = \langle n/2 \rangle$,

$$x^t + u_t(x) + 1 \neq w_i(x) \qquad t = 1, 2, \ldots \langle n/2 \rangle .$$

Now,

$$u_t(x) + 1 = u_t(x), \qquad \text{a symbolic equality.}$$

Thus,

$$x^t + u_t(x) \neq w_i(x) \qquad t = 1, 2, \ldots \langle n/2 \rangle \qquad (2.23)$$

It is certainly clear that Eq. (2.23) must hold for $w_i(x) =$ the codeword of all 0's. Now if $w_i(x)$ is a nonzero codeword, at least one of the information digits, i.e., at least one of the coefficients of a power of x of degree n-k-1 or higher, must be nonzero. But the left side of Eq. (2.23) has no power of x greater than $t \leq \langle n/2 \rangle$. Therefore, Eq. (2.23) will be satisfied if:

$$\langle n/2 \rangle < n\text{-}k\text{-}1$$

or

$$k < \langle n/2 \rangle \qquad \text{Q.E.D.}$$

In the next section are described the ρ-repetition altered cyclic codes, which permit the attainment of high degrees of comma freedom.

2.2.3 The ρ-Repetition Cyclic Codes

We shall now devise a method of construction of an interesting class of codes capable of providing various values of (s, δ) including $s = \langle n/2 \rangle$.

To every (n, k) cyclic code generated by the polynomial $g(x)$, there corresponds the $(\rho n, k)$ ρ-repetition cyclic code generated by the polynomial: $g(x)\,[1 + x^{n} + x^{2n} + \ldots + x^{\rho n - n}]$. Each word in this new code consists of a ρ-fold repetition of the corresponding word in the original code. Any n consecutive digits are identical to the next n (cyclically) consecutive digits. If the original code has a minimum distance d between codewords, the repetition code has a distance ρd. Furthermore, the repetition code is capable of correcting any burst of errors of length $\begin{cases} \leq (\frac{\rho}{2} - 1)\, n - 1, & \rho \text{ even} \\ \leq \frac{(\rho - 1)n}{2} + 1, & \rho \text{ odd} \end{cases}$. These error-correcting properties are of course unchanged by the addition of $r(x)$.

Let us picture the vector $r(x)\,[x^{t} + 1] + u_{t}(x)$ appearing in Eq. (2.22).

A	B	C
$\leftarrow \rho n - [t + z + 1] \rightarrow$	$\leftarrow z + 1 \rightarrow$	$\leftarrow t \rightarrow$

Section A of the vector consists of $\rho n - [t + z + 1]$ 0's. The $z + 1$ places of Section B are that part of $r(x)\,[x^{t} + 1]$ of degree $\geq t$. Section C represents t arbitrary digits picked up from an adjacent codeword. Equation (2.22) states that for the altered code to have the characteristic (s, δ) for all $t = 1, 2, \ldots s$, we must have to change at least δ digits to transform this vector into a valid codeword.

Suppose that an $r(x)$ is chosen such that the weight of the $z + 1$ digits of Section B is at least δ. Suppose further that $\rho n - [s + z + 1] \geq n$ and $\rho n - [s + z + 1] \geq z + 1$. Section A must contain within itself a replica of Section B if there is to be any possibility of the vector forming a valid codeword. This could occur as a result of any of several types of error patterns: the wiping out of δ 1's in Section B; the wiping out of δ-1 1's in Section B and the placement of a 1 in Section A; the wiping out of δ-2 1's in Section B and the placement of two 1's in Section A; . . . . But no error pattern of weight $\delta - 1$ or less will achieve this. Thus, we can state the following theorem:

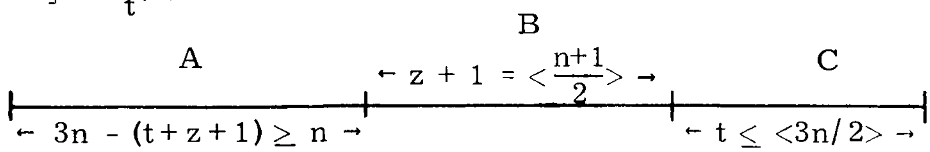
Theorem II

If a ρ-repetition $(\rho n, k)$ cyclic code is altered by the addition of $r(x)$ where z is the degree of $r(x)$, and the weight of that part of $r(x)\,[x^t+1]$ of degree $\geq t$ is at least δ, then if: $\rho n - [s + z + 1] \geq n$ and $\rho n - [s + z + 1] \geq z + 1$, the resultant altered code will have the characteristic (s, δ).

Below are discussed two classes of ρ-repetition altered cyclic codes possessing $s = < n/2 >$ (complete comma freedom) and various values of δ. It should be clear from these examples how similar codes could be constructed for larger ρ.

a) $\rho = 3$; threefold repetition of an (n, k) code.

These codes have a block length of 3n; $s = <3n/2>$. The vector $r(x)\,[x^t + 1] + u_t(x)$ is:



Following are tabulated some possible codes generated.

Block Length 3n	δ	r(x)
15	2	$x + x^2$
27	3	$1 + x^2 + x^3 + x^4$
39	4	$x + x^4 + x^5 + x^6$
51	5	$x + x^4 + x^6 + x^7 + x^8$
62	6	$x^2 + x^4 + x^7 + x^8 + x^9 + x^{10}$

b) $\rho = 4$; fourfold repetition of an (n, k) code.

The appropriate picture of $r(x)\,[x^t + 1] + u_t(x)$ is now:

A | B | C

$\leftarrow 4n - [t + z + 1] \geq n \rightarrow \leftarrow z + 1 = n \rightarrow \leftarrow t \leq 2n \rightarrow$

Some possible codes are:

Block Length 4n	δ	r(x)
12	2	$x + x^2$
20	3	$1 + x^2 + x^3 + x^4$
28	4	$x + x^4 + x^5 + x^6$
36	5	$x + x^4 + x^6 + x^7 + x^8$
44	6	$x^2 + x^4 + x^7 + x^8 + x^9 + x^{10}$

It is perhaps not apparent from Theorem II that the choice of r(x) effects, for a given code, a trade-off between s and δ. The table below shows the various possible combinations (s, δ) and the corresponding r(x) for two codes.

$r(x)$	$\rho = 2$ $\rho n = 14$	$\rho = 3$ $\rho n = 21$
1	(6, 1)	
$x + x^2$	(4, 2)	(10, 2) (completely comma-free δ=2)
$1 + x^2 + x^3 + x^4$	(2, 3)	(9, 3)
$x + x^4 + x^5 + x^6$		(7, 4)
$x + x^4 + x^6 + x^7 + x^8$		(3, 5)

Let us note in conclusion that the self-synchronizing properties of these ρ-repetition altered codes depend only upon the block length n of the (n, k) code used to build it up. The (28, 7) altered code built from quadruple repetition of the trivial (7, 7) code will, when synchronism is held, correct all bursts of length 7 or less, and has a minimum distance of 4. The (28, 4) code built from the (7, 4) single-error-correcting code has a minimum distance of 12, and will correct bursts of length 8 or less. But both codes will be completely comma-free with $\delta = 4$.

A word of caution is in order concerning the combined error-correction and synchronization-loss detection properties of these codes. The (28, 4) code, which can correct quintuple errors when in synchronism, might easily mistake loss of synchronism for a quadruple error and "correct" an overlap sequence into a wrong word instead of reframing it. With a code of comma freedom δ, the decoder must, therefore, be designed to correct no more than δ errors. Even this does not completely solve the problem since a combination of synchronization slip and errors could produce what appears to be a "correctable" codeword. In the case of error detection only, this question does not arise, but if error correction is to be considered the interplay of overlaps and errors must be studied in more detail.

2.2.4 Probability of Undetected Loss of Sync for ρ-Repetition Codes

Let us consider the vector that must not be equal to a codeword in the original cyclic code if the loss of synchronism is to be detected.

Section A consists of $n - [t + z + 1]$ 0's, Section B is that part of $r(x)\,[x^t + 1]$ of degree $\geq t$ and has at least δ 1's in it; $u_t(x)$ is an arbitrary sequence picked up from an adjacent codeword. A necessary but not sufficient condition for undetected loss of synchronization to occur is that those $z + 1$ digits of Section A lying n digits ahead of Section B must match with Section B in all $z + 1$ places.

We assume that individual digit errors occur independently with probability p. We can now get an upper bound to P, the probability of undetected loss of synchronism.

Let us enumerate the subclasses into which error patterns causing undetected loss of synchronism may fall:

No errors in Section B, δ or more errors in Section A

1 error among the δ or more 1's in Section B;
δ-1 or more errors in Section A,

2 errors among the δ or more 1's in Section B;
δ-2 or more errors in Section A,

$\vdots$

δ errors among the δ or more 1's in Section B;
errors in Section A.

Besides this, the other places in the sequence must coincide with those of a valid codeword. The arbitrary vector $u_t(x)$ assumes the right value with

$$\text{probability} \begin{cases} 2^{-t}, & t < k \\ 2^{-k}, & t \geq k \end{cases}$$

The positions in Sections A and B not covered above assume the right value with a probability < 1. Thus, an upper bound to the probability of undetected loss of synchronization is

$$P < [p^{\delta} + p \cdot p^{\delta-1} \binom{\delta}{1} + p^2 p^{\delta-2} \binom{\delta}{2} + \ldots + p^{\delta} \binom{\delta}{\delta}] \; 2^{-t} \quad t \leq k$$

$$P < [p^{\delta} + p \cdot p^{\delta-1} \binom{\delta}{1} + p^2 \cdot p^{\delta-2} \binom{\delta}{2} + \ldots + p^{\delta} \binom{\delta}{\delta}] \; 2^{-k} \quad t \geq k.$$

or

$$P < (2p)^{\delta} \; 2^{-t} \qquad t \leq k$$

$$P < (2p)^{\delta} \; 2^{-k} \qquad t \geq k.$$

When $\delta = 0$ this bound gives the well-known result for a cyclic code that the probability of undetected slip decreases as 2^{-t} where t is the amount of overlap. This factor is present even when slip detection of degree δ is designed into the code. The major purpose of the slip detection alteration of cyclic codes is to reduce P when the slip t is small.

2.3 Use of Telemetry Systems for Command Verification

2.3.1 Introduction

The feedback mode of operation requires that there exists a link from the space vehicle to the ground. Such a link is already available in the telemetry system. It therefore appears attractive to use part of the capacity of this already existing link for the feedback information. From an operational point of view there are a number of obstacles to the straightforward utilization of the telemetry link. These difficulties are generally of three types.

a) The telemetry system is already fully loaded with data.

b) The telemetry system was not designed with this feedback application in mind and it is therefore difficult in many cases to incorporate this feature later.

c) The telemetry transmission rate may be so slow as to be unsuitable for feedback.

The spectrum of existing systems ranges all the way from the fully integrated Apollo system where all ranging updata and telemetry problems have been solved by use of only one system to the OAO satellite which has a telemetry system with a bit rate of only 1.042 kb/sec. It is therefore necessary to study several typical systems in order to get a more general picture of the situation. We will choose the OAO, the OGO, the TIROS and the APOLLO spacecraft as representative examples.

2.3.2 OAO Satellite

Two interdependent telemetry systems are employed on the OAO satellite to reorganize digital and analog signals into a standard output format. One is the Spacecraft Data Handling Equipment (SDHE). This system is synchronized to the spacecraft gimbal command information and monitors performance. The second system, the Experimenters Data Handling

Equipment, is an asynchronous system that monitors the various experiments conducted within the spacecraft. A block diagram of the OAO data processing system is shown in Fig. 1.

A primary feature of the OAO is its ability to react in response to a variety of ground commands. In addition to experiment commands, by which a ground-based operator can exercise control over the astronomical equipments, the OAO can also be sent a variety of spacecraft commands.

Commands are received from the ground, decoded, and sent to the proper destination within the observatory by means of a command decoder and distributor. Data gathered by the experiment and spacecraft status data are stored in a magnetic core data storage unit. A data programmer adds synchronization to the data frames as data is programmed out of storage and transmitted. If the amount of generated data at one instant exceeds the capacity of the telemetry system, this data can be placed in storage for transmission at a later time.

For an understanding of the operation of the SDHE it is necessary first to study the word format in use. Figure 2 shows the SDHE serial output format for real time transmission. Each frame consists of 65 words and lasts 1.6 sec. Each word consists of 26 bits. The real time bit rate is 1.042 kb/sec. Each frame consists of:

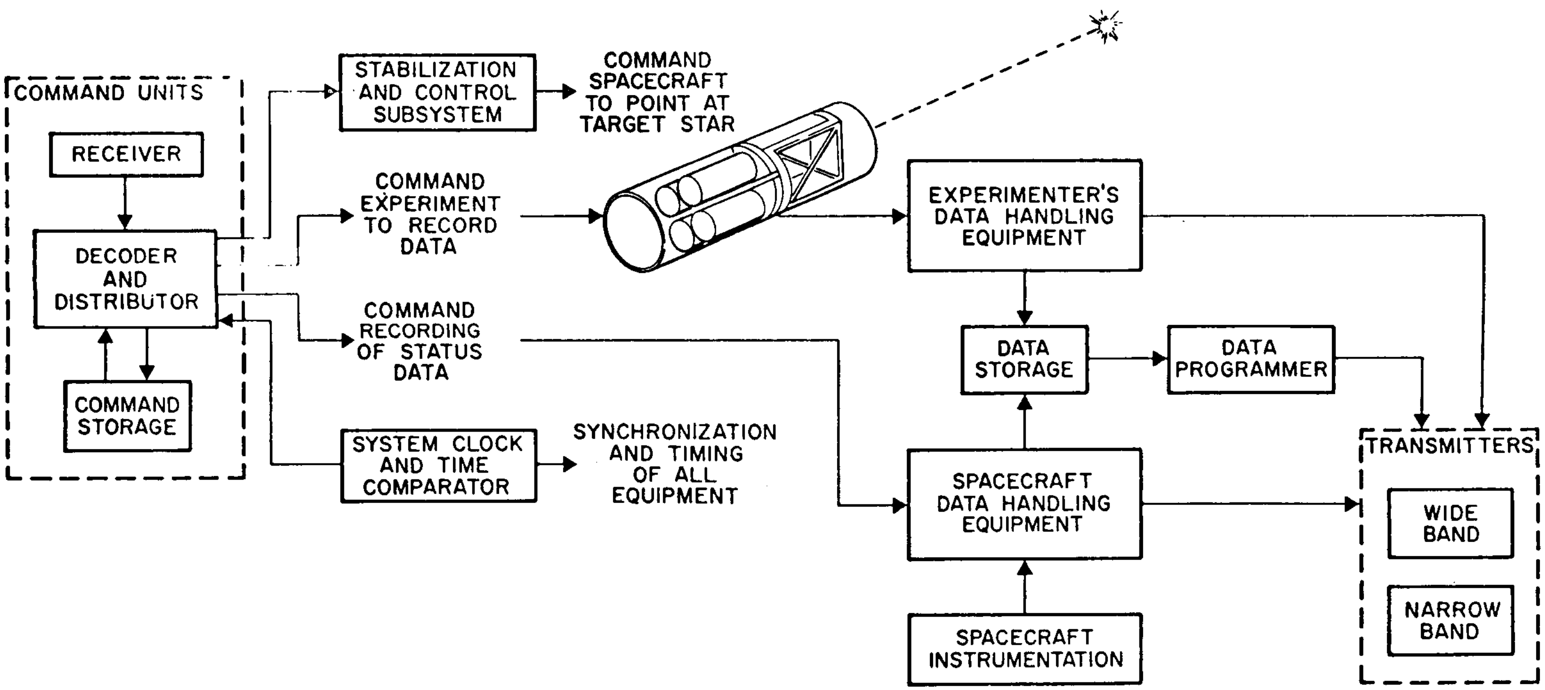


Fig. 1 OAO data processing and instrumentation.

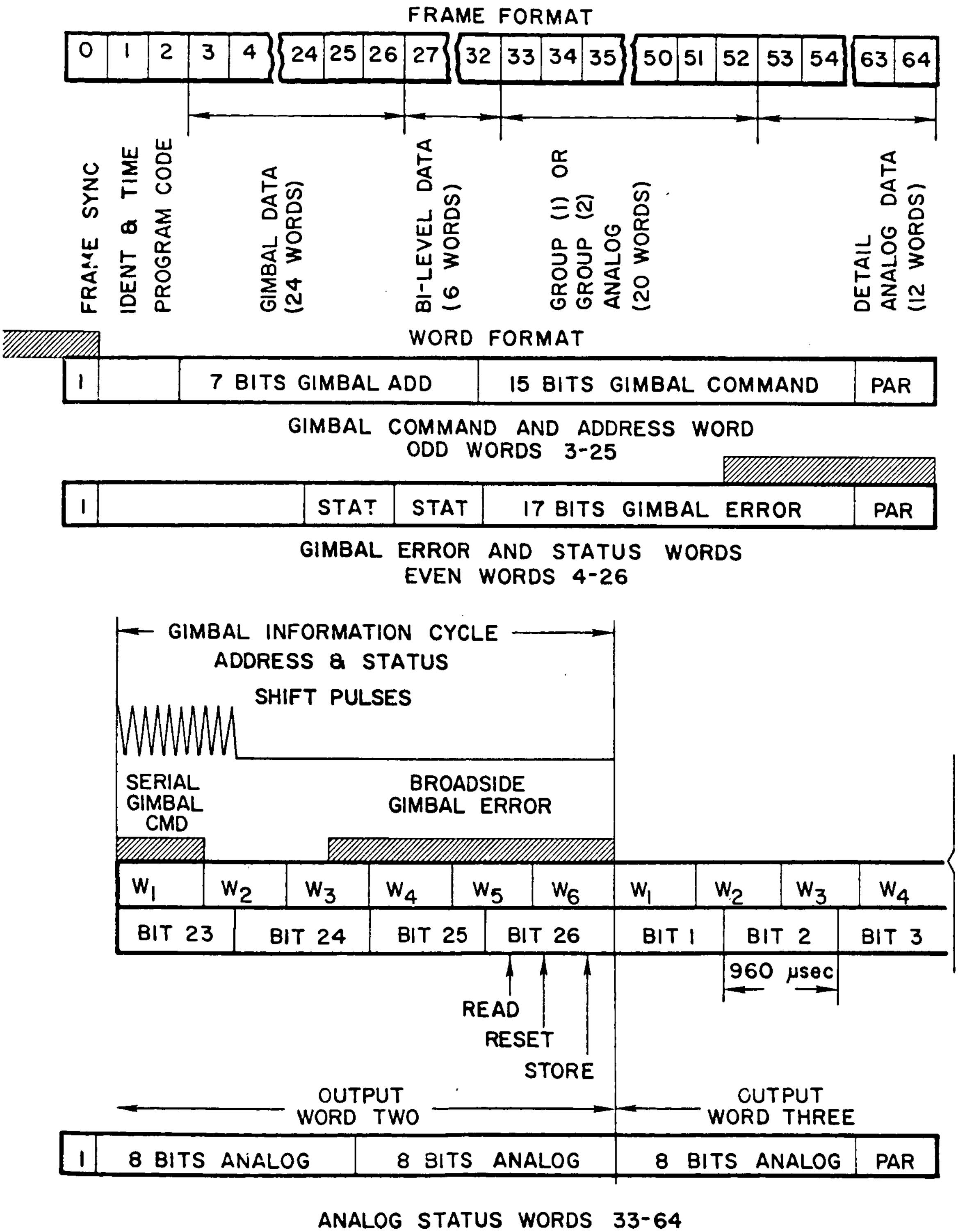


Fig. 2 Real time output format.

1. Word Zero. Frame sync.
2. Word One. Transmission time in a 10 bit binary code.
3. Word Two. The SDHE command word address.
4. Words 3 through 26. Gimbal monitoring information. There are 6 inner and 6 outer gimbals to monitor. Two words are required to display one set of gimbal information. Since system performance is centered around the ability to display gimbal information correctly, the SDHE is synchronized with the gimbal input cycles.
5. Words 27 through 32. Words containing six groups of bi-level information with 25 channels per group. There are eight groups of bi-level channels available and the unit may be commanded to select alternate groups.
6. Words 33 through 64. These are words containing eight bit coded measurements of analog input channels. Three channel measurements are contained in each output word. Any combination of analog channel groups may be programmed by the unit address command.

Now that we know the word format and bit rates we may start to inquire into the real question. Is it possible to use some fraction of the telemetry capacity of the SDHE for feedback verification? Whether this is possible or not depends mainly on three factors:

a) amount of feedback needed,
b) present loading on the telemetry equipment, and
c) possible modification of the telemetry format without significant reduction in telemetry performance.

To the last category belongs an alternative that may be possible but which will not be considered in this section: that is, injecting the feedback signal on a subcarrier into the modulator of the telemetry transmitter. As an illustration assume that commands are sent at a rate of 10 per sec and that a five-bit code is required for each verification, including address. We see that a feedback rate of 50 bits/sec is required. It is undesirable to store the feedback information before transmission since this only increases the total loop delay. It is therefore desirable that five bits are made available every 100 msec for the feedback information. Since each word is 24.8 msec in duration this means that five bits in every fourth word will be taken up by feedback information. This reduces the capacity of the telemetry system by less than 4.8 % which should certainly not be an intolerable reduction.

We meet the first real stumbling block in the gimbal information words. They constitute 24 consecutive words which require 590 msec for transmission. This represents a serious obstacle that may perhaps be overcome by a slight change in gimbal address format. This can be better understood with reference to Fig. 2. Two successive words contain the necessary information about one gimbal. The first word contains gimbal address and command condition. Gimbal address has a one in one of the first six bit position to indicate gimbal number. The seventh bit indicates whether it is an inner or an outer gimbal. "STAT" indicates lock on for the particular star tracker associated with the gimbal being monitored. The gimbal address can easily be compressed from seven to four bits by using a regular binary code for the 12 different gimbals. This frees three bits per two words or six bits for each command verification.

Command verification "subwords" can be inserted in word one since 10 bits of it are used to transmit the transmission time. The words that could contain command verification are therefore words 1, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 31, 35, 39, 43, 47, 51, 55, 59, 63. No problems are expected with words 27 and 31 since they consist of 25 binary input channels. The coding on channels 35, 39, 43, 47, 51, 55, 59 and 63 will have to be rearranged if full use is to be made of them. Since the feed-back code was assumed to be only five bits in duration the remaining three bits on the relevant channels can be used for other purposes. One could, for instance, use them as three additional bi-level inputs or one could use them as three bit-coded analog channels.

If a method following the pattern here is used for the updata feedback link a considerable improvement in the vitally important updata link can be realized. This can be achieved at a cost of only 1.92 % reduction in telemetry rate.

2.3.3 OGO, POGO, and EGO Satellites

The Orbiting Geophysical Observatory is a standardized earth satellite that can fly as many as 50 experiments per mission in a wide range of orbits. Two particularly interesting missions are the EGO (Eccentric Orbiting Geophysical Observatory) and the POGO (Polar Orbiting Geophysical Observatory). The EGO mission has a perigee of 278 km and an apogee of 115, 000 km while the POGO mission has an apogee of 259 km and a perigee of 926 km. Since both missions use the same basic 4 watt telemetry transmitter, we see that an adaptive system is indicated if one wants to utilize the available transmitter power efficiently. The EGO telemetry system can operate at bit rates of 64, 8 and 1 kbits/sec. The POGO satellite does not have to decrease its bit rate as much as the EGO since it is closer to the earth at its apogee. Its telemetry system can operate at 64, 16 and 4 kbits/sec. It seems doubtful whether the 4 kbits/sec rate is needed on this mission.

The command decoder operates at a bit rate of 128 bits/sec. The command decoder operates the command distribution unit. This unit consists of a 16 × 16 relay matrix providing a total of 254 commands. The first and last command of the relay matrix are not utilized in the system.

The command word contains 24 bits. The first bit in the command word is a one for sync. The next three bits are used for address. Since it is required that at least one of these three bits be a one the system has the capability of addressing up to seven different decoders. The next two bits are used to switch the mode in which the command system shall operate. The next eight bits provide the 254 commands. The two mode switching bits and the eight command bits are then repeated in an inverted position and checked in the digital decoder before any of the relays in the command distribution unit are activated. Each command word has a duration of 0.188 sec. Since a command verification word should be fed back as soon as the spacecraft receiver has made a decision on the received word,

• a feedback word should be inserted in the telemetry frame each 0.188 sec.

The basic telemetry format consists of 128 nine-bit words in the main frame. Since the bit rates of the telemetry system can vary between 64,000 and 1,000 bits/sec while the command rate remains fixed, the most efficient solution is an adaptive format. This can be accomplished relatively simply since the rates used are all quaternary multiples of the lowest telemetry bit rate. During the time it takes for reception of one command word the telemetry system, working at its slowest rate, has transmitted

$$\frac{24,000}{128} = 187.5 \text{ bits}$$

In order for the command and telemetry systems to keep in step a feedback word should be inserted into the telemetry frame every 187.5 bits when the telemetry system is operating at its lowest rate. Since half bits do not exist we can use 187 and 188 telemetry bits alternately between the feedback words. This problem vanishes for all but the lowest telemetry rate.

In order to fit the feedback words in smoothly to the telemetry format we must also take account of the periodicity of the telemetry words. Since each word consists of nine bits, 20.833 words are transmitted during the time it takes to receive one command word. Figure 3 shows the main frame format. We will assume that the first few bits of word 9 are used for feedback verification. Each line in the frame contains 144 bits. Since 188 bits are required between feedback words for efficient utilization of the available transmission capacity, the location of the feedback words should move around within the frame. This is very undesirable from an operational

	K101	K102	K103	K104	K105	K106	K107	K108	K109	K110	K111	K112	K113	K114	K115	K116
R11	1	2	3	4 A	5 A	6 A	7 A	8 A	9 D	10 D/A	11 D/A	12 D/A	13 A	14 A	15 A	16 A
R12	7 D	18 D	19 D	20 D/A	21 A	22 A	23 A	24 A	25 D	26 D/A	27 D/A	28 D/A	29 A	30 A	31 A	32 A
R13	33 Accumulated Time (Secs)	34	35	36 A	37 A	38 A	39 A	40 A	41 D	42 D/A	43 D/A	44 D/A	45 A	46 A	47 A	48 A
R14	49 D	50 D	51 D	52 D/A	53 A	54 A	55 A	56 A	57 D	58 D/A	59 D/A	60 D/A	61 A	62 A	63 A	64 A
R15	65 Identification Words — Data Being Examined: SUB-COMMUTATOR POSITION	66 MODE, FLEXIBLE FORMAT NO. 1	67 Data Not Examined: MODE, FLEXIBLE FORMAT NO. 2	68 A	69 A	70 A	71 A	72 A	73 D	74 D/A	75 D/A	76 D/A	77 A	78 A	79 A	80 A
R16	81 D	82 D	83 D	84 D/A	85 A	86 A	87 A	88 A	89 D	90 D/A	91 D/A	92 D/A	93 A	94 A	95 A	96 A
R17	97 Experiment Sub-Commutator	98 Spacecraft Sub-Commutator No. 1	99 Spacecraft Sub-Commutator No. 2	100 A	101 A	102 A	103 A	104 A	105 D	106 D/A	107 D/A	108 D/A	109 A	110 A	111 A	112 A
R18	113 D	114 D	115 D	116 D/A	117 A	118 A	119 A	120 A	121 D	122 D/A	123 D/A	124 D/A	125 A	126 A	127 A	128 A

D = Digital Experiment
A = Analog Experiment
D/A = Digital or Analog Experiment

Fig. 3 Main telemetry frame format OGO satellite. Proposed location of feedback verification words shown.

point of view. Since approximately 6.14 feedback words are required per frame, it seems reasonable to insert an equalization word to make a total of seven feedback words in the telemetry frame. A suggested arrangement of feedback words is shown in Fig. 3. As the bit rate is increased, the number of feedback words can be reduced. At a bit rate of 4 kbits/sec only two feedback words per frame are required. For higher transmission rate, one feedback word per frame will be sufficient.

III. PROGRAM FOR NEXT REPORTING INTERVAL

The effect of uplink and downlink channel characteristics on data rate will be investigated for various feedback strategies.

System integration problems will be studied, including the use of a ground-based data handling computer for real-time control and for simulation.

Recommendations will be made for appropriate system parameters using both present standard equipments and more advanced techniques.

IV. CONCLUSIONS AND RECOMMENDATIONS

a) One meaningful measure of error-detecting system performance is the probability, P_e, of an accepted codeword being in error. This error probability depends only on the uplink characteristics and on the code structure, but not on the feedback link. For a binary symmetric channel with transition probability p, P_e can be calculated from the codeword weight distribution, W(i), or from its approximation according to Eqs. (2. 2), (2. 6) and (2. 18).

b) Cyclic codes for error detection can be altered to detect loss of synchronization by the addition of a fixed binary vector to each codeword prior to transmission. These codes are characterized by a pair of numbers (s, δ) such that a synchronization slip of s bits can be detected whenever each codeword contains less than δ errors. Multiple repetitions of cyclic codewords, appropriately altered, permit a considerable range of s and δ at some sacrifice in data rate.

c) Telemetry formats must be adapted to accept feedback information from the updata link. Feedback will in general demand only a small percentage of downlink capacity, but the allocation of this capacity will require appropriate design of telemetry formats to provide timely access to the downlink.

V. REFERENCES

1. Peterson, W. W., Error-Correcting Codes, Wiley and Sons, N. Y., 1961, p. 47.

2. Nesenbergs, M., "Comparison of the 3-out-of-7 ARQ with Bose-Chandhuri-Hocquenhem Coding Systems," IRE Trans. on Comm. Syst., CS-8, March 1960.

3. Corr, F. P., "A Statistical Evaluation of Error Detection Cyclic Codes for Data Transmission," IEEE Trans. on Comm. Syst., CS-12, June 1964.

4. Elliot, E. O., "Estimates of Error Rates for Codes on Burst-Noise Channels," Bell Syst. Tech. J., v. 42, September 1963.